



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/805,429

03/19/2004

Sebastian J. Hans

P-8729

9180

24209

7590

03/07/2008

GUNNISON MCKAY & HODGSON, LLP
1900 GARDEN ROAD
SUITE 220
MONTEREY, CA 93940

EXAMINER

OKORONKWO, CHINWENDU C

ART UNIT

PAPER NUMBER

2136

MAIL DATE

DELIVERY MODE

03/07/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 12/17/2007, the following claims, claims 1-100 are presented for examination.

Response to Remarks/Arguments

2. Applicant's arguments, pages 20-23, with respect to the rejection of claims 1-100 have been fully considered but they are not persuasive.

2.1 In response to Applicant argument that the Bacha et al. (Bacha) reference does not teach or suggest "that processes that utilize the memory and computing resources and work stations could be implemented on a card device," the Examiner respectfully disagrees citing column 5 lines 47-49 and lines 64-65 which clearly recites, "the document repository system 204 of the preferred embodiment comprises two components, an application server 210 and a vault controller 214. The application server is a program to administer the database repository 212, which may be on the same machine or may be remotely located on a closed network," and "the application server component 210 does not run on a trusted computing base, but can execute on any platform." Thus the Examiner understands the application server program to be executable on "any platform" including on the claimed "card device" and or on various operating systems. The rejection has not been overcome, therefore the rejection of claims 1-100 is maintained.

Claim Rejections - 35 USC § 103

- 3 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-100 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bacha et al. (US Patent No. 6839843 A1) and further in view of Riddle (US Patent No. 5,572,582).

Regarding claims 1, 25, 49 and 73, Bacha et al., discloses a card device for communication with an electronic device, comprising: a capabilities list associated with an application program, said capabilities list including information regarding access to one or more resources for use by said application program, and for storing said application program and a security manager (col. 2 lines 51-67 and col. 3 lines 1-24 – “data repository” equated to capabilities list, “agent program” equated to application program and “repository manager” equated to security manager); and said security manager, said security manager for selectively granting access to said one or more resources for use by said application program based at least in part on said capabilities list (col. 2 lines 51-

67 and col. 3 lines 1-24—"authenticating user access to electronic data stored in a data repository managed by a repository manager " equated to granting access to said one or more resources).

Bacha et al. is silent in disclosing a memory for storage and a processor for executing said application program, however Riddle does disclose such elements (col. 4 lines 12-32 of Riddle - "a random access memory (RAM) or other volatile storage device 304 (referred to as main memory), coupled to bus 301 for storing information and instructions to be executed by processor 302.").

It would have been obvious to one of ordinary skill to have combined the system for electronic repository of data enforcing access control on data retrieval with the method and apparatus for establishing communication between two teleconferencing endpoints to use a memory source and processor. Riddle provides motivation for the combination in the recitation of "a general purpose computer system us used for implementing the teleconferencing application and associated processes" such as the ones contained within the claim invention (col. 4 lines 1-11).

Regarding claims 2, 26, 50 and 74, Bacha et al., discloses the card device of claim 1 wherein said one or more resources comprise at least one of data and

functions (col. 3 lines 3-15 – “system and method for securely authenticating user access to electronic data stored in a data repository ... the source is responsible for updating the access control list , and maintains evidence of the current access control list.”).

Regarding claims 3, 27, 51 and 75, Bacha et al., discloses the card device of claim 1 wherein said one or more resources comprise one or more resources external to said card device (Figure 1, col. 2 lines 52-60 and col. 7 lines 25-41 – “secure electronic data (document)” and “encrypted document ... are all stored in the application;s server’s repository or the application database.”).

Regarding claims 4, 28, 52 and 76, Bacha et al., discloses the card device of claim 3, further comprising at least one of: terminal side resources and channels of a communications network (Figure 4).

Regarding claims 5, 29, 53 and 77, Bacha et al., discloses the card device of claim 1 wherein said one or more resources comprise one or more resources owned by at least one of said application program and another entity (col. 8 line 64 - col. 9 lines 26 – “in a data repository there is a requirement for document access control ... only those users authorized by the document’s owner, are able to view the document.”).

Regarding claims 6, 30, 54 and 78, Bacha et al., discloses the card device of claim 5 wherein said other entity comprise at least one of: an operating system of said card device and another application program (column 5 lines 47-49 and lines 64-65 – “the application server component does not run on a trusted computing base, but can execute on any platform.”).

Regarding claims 7, 31, 55 and 79, Bacha et al., discloses card device of claim 1 wherein said capabilities list comprises information regarding at least one of: access rights; and information required for access to a resource (Figure 2 and col. 3 lines 3-14 – “access control list of user authorizations is associated with the electronic data when stored in the data repository.”).

Regarding claims 8, 32, 56 and 80, Bacha et al., discloses the card device of claim 1 wherein said memory stores a first capabilities list and a second capabilities list, said first capabilities list comprising a handle to link to said second capabilities list (col. 11 lines 21-31 – “the data that needs to be included in a backup are ... the capabilities lists.”).

Regarding claims 9, 33, 57 and 81, Bacha et al., discloses the card device of claim 8 wherein said second capabilities list is associated with one or more of other application programs (col. 11 lines 21-31 – “the data that needs to be

included in a backup are ... the capabilities lists (for the systems [that] implement them, as described above), and the verification tokens of ACLs and capability lists”).).

Regarding claims 10, 34, 58 and 82, Bacha et al., discloses the card device of claim 1 wherein said application program is for requesting access to a resource (col. 8 lines 3-43 – “access request”).

Regarding claims 11, 35, 59 and 83, Bacha et al., discloses the card device of claim 1 wherein said application program is for transmitting a resource access request to a security manager (col. 2 lines 51-67 and col. 3 lines 1-24); and said security manager is for transmitting a verify request to a verification program to examine said capabilities list to determine whether said application program is authorized to access said resource, and for performing or denying said requested action based at least in part on said examination (col. 2 lines 51-67 and col. 3 lines 1-24).

Regarding claims 12, 36, 60 and 84, Bacha et al., discloses the card device of claim 11 wherein said security manager comprises an application program interface (API) (col. 5 lines 1-31 – “this is done through an API”).

Regarding claim 13, 37, 61 and 85, Bacha et al., discloses the card device of claim 11 wherein said security manager is for obtaining information regarding said requesting application program through one of inquiring at a context originating the resource access request and a parameter provided with said resource access request (col. 2 lines 52-60 and col. 7 lines 25-41 – “repository manager for managing storage and retrieval of encrypted electronic data” and “non-repudiation receipt” is equated to the parameter).

Regarding claim 14, 38, 62 and 86, Bacha et al., discloses the card device of claim 1, further comprising input/output means for receiving said capabilities list from at least one of a provider of said application program and an owner of said one or more resources (col. 2 lines 52-60 and col. 7 lines 25-41).

Regarding claim 15, 39, 63 and 87, Bacha et al., discloses the card device of claim 1 wherein said capabilities list and said application program constitute a load package received by said card device (Figure 2 and col. 3 lines 3-14).

Regarding claims 16, 40, 64 and 88, Bacha et al., discloses the card device of claim 1 wherein said device is configured to modify said capabilities list based at least in part on a subsequently received capabilities update list associated with said application program (Figure 2, col. 3 lines 3-14 and col. 11 lines 21-31).

Regarding claims 17, 41, 65 and 89, Bacha et al., is silent in disclosing the card device of claim 1 wherein said device is configured to delete said capabilities list or link and access rights upon receiving an instruction to delete said application program from the outside, however Riddle does disclose such elements (col. 20 lines 20-47 – “entities are deleted”).

It would have been obvious to one of ordinary skill to have combined the system for electronic repository of data enforcing access control on data retrieval with the method and apparatus for establishing communication between two teleconferencing endpoints to use a memory source and processor. Riddle provides motivation for the combination in the recitation of “a general purpose computer system us used for implementing the teleconferencing application and associated processes” such as the ones contained within the claim invention (col. 4 lines 1-11).

Regarding claims 18, 42, 66 and 90, Bacha et al., discloses the card device of claim 1 wherein said capabilities list is encrypted; and said processor is configured to decrypt said capabilities list (col. 6 lines 28-60).

Regarding claims 19, 43, 67 and 91, Bacha et al., discloses the card device of claim 1 wherein said capabilities list is cryptographically signed by at least one of

a provider of said application program and an owner of said one or more resources (col. 6 lines 28-60); and said processor is configured to cryptographically authenticate said capabilities list (col. 6 lines 28-60).

Regarding claims 20, 44, 68 and 92, Bacha et al., discloses the card device of claim 19 wherein said processor is further configured to cryptographically authenticate said capabilities list when said capabilities list is stored on said device (col. 6 lines 28-60).

Regarding claims 21, 45, 69 and 93, Bacha et al., discloses the card device of claim 19 wherein said processor is further configured to cryptographically authenticate said capabilities list when said capabilities list is accessed, said capabilities list being successfully authenticated if a first fingerprint computed over said capabilities list upon storing capabilities list matches a second fingerprint computed over said capabilities list in response to a run-time request to use said capabilities list (col. 6 lines 28-60).

Regarding claims 22, 45, 70, 94, Bacha et al., discloses the card device of claim 1 wherein said application program comprises a plurality of modules (Figures 4, 4A and 4B).

Regarding claims 23, 46, 71, 95, Bacha et al., discloses the card device of claim

Art Unit: 2136

1 wherein said application program comprises a Java application program or a Java Card.TM. applet (col. 12 lines 23-39).

Regarding claims 24, 47, 72, 96, Bacha et al., discloses the card device of claim 1 wherein said capabilities list is embodied in a tag-length-value (TLV) structure (col. 2 lines 51-67 and col. 3 lines 1-24).

Regarding claims 97, Bacha et al., discloses a memory for storing data for access by an application program being executed on a data processing system, comprising: a data structure stored in said memory, said data structure including information used by said application program to determine at run-time information regarding access to one or more resources for use by said application program (col. 2 lines 51-67 and col. 3 lines 1-24).

Regarding claims 98, Bacha et al., is silent in disclosing a memory of claim 97 wherein said memory is for storing said application program and said data structure, however Riddle does disclose such elements (col. 4 lines 12-32 of Riddle – “a random access memory (RAM) or other volatile storage device 304 (referred to as main memory), coupled to bus 301 for storing information and instructions to be executed by processor 302.”).

It would have been obvious to one of ordinary skill to have combined the system for electronic repository of data enforcing access control on data retrieval with the method and apparatus for establishing communication between two teleconferencing endpoints to use a memory source and processor. Riddle provides motivation for the combination in the recitation of “a general purpose computer system us used for implementing the teleconferencing application and associated processes” such as the ones contained within the claim invention (col. 4 lines 1-11).

Regarding claims 99, Bacha et al., discloses a memory of claim 98 wherein said application program and said data structure are contiguous in said memory (col. 8 lines 3-43).

Regarding claims 100, Bacha et al., discloses a memory of claim 98 wherein said data structure is stored within said application program in said memory (col. 8 lines 3-43).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

Art Unit: 2136

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./

Examiner, Art Unit 2136

March 12, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136